RSAC 2025 Conference

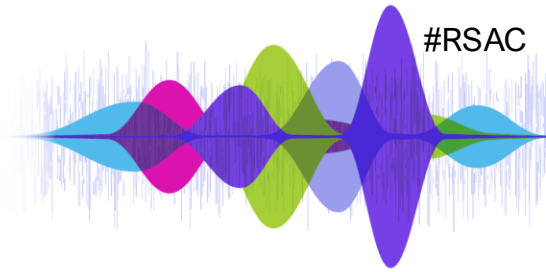
Many Voices.
One Community.

SESSION ID: IMT-T01

Creating Calm in the Storm: Weathering the Cyber Sharknado

Sydney Delp

Director of Defense Operations
Target Corporation



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

2013

Target: 40 million credit cards compromised

by CNNMoney Staff @CNNMoney

December 19, 2013: 4:41 PM ET

ATM | BINS | BITCOIN | CARD SHOP | DUMPS | LITECOIN | MASTERCARD | MONEYGRAM | PERFECTMONEY | PIN | TARGET | TARGET CREDIT CARD HACK | TARGET DATA BREACH | TORTUGA | TORTUGA BASE | VISA | WEBMONEY | WESTERN UNION

Sources: Target Investigating Data Breach

December 18, 2013 620 Comments

Nationwide retail giant Target is investigating a data breach potentially involving millions of customer credit and debit cards stolen from physical stores over the past few weeks, multiple reliable sources tell KrebsOnSecurity.

Forty Million Target Customers Affected By Data Breach

By Kelly Clay, Former Contributor. I write about social media, startups and technology trends.

Dec 18, 2013, 05:57pm EST

'Sharknado' keeps TV real

By Mary McNamara

July 11, 2013 10:17 AM PT

'Sharknado' Dares To Ask: Is It Going To Rain Giant Man-Eating Sharks?

JULY 12, 2013 · 8:35 AM ET

Linda Holmes

Regular Sharknado

Is someone helping the injured??

When will power be restored?

Are the roads cleared for EMTs?

We need to tell people to stay indoors!!!

Some of these sharks are still alive!!

Cyber Sharknado

What do we say to the media?

Which systems are we prioritizing getting back up?

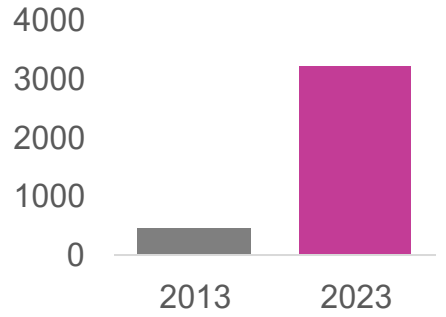
Where are we at with containment?

What're our disclosure obligations?

Is this incident considered material?

Why is this relevant?

Cyber sharknados are increasingly common…

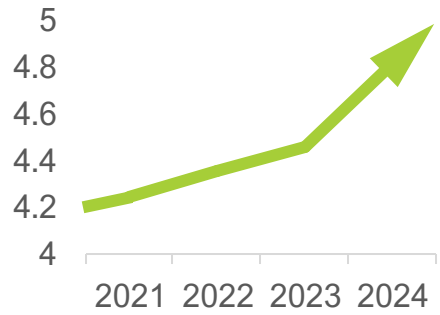


600%+

increase in # of known data breaches

since 2013

…and increasingly expensive

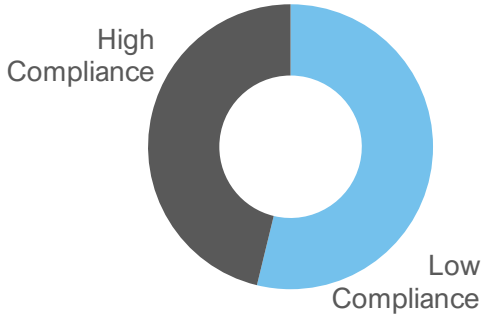


$4.8mil

Average cost of a data breach in 2024

Up 10% since 2023

…especially when mishandled



12%

Higher costs on avg

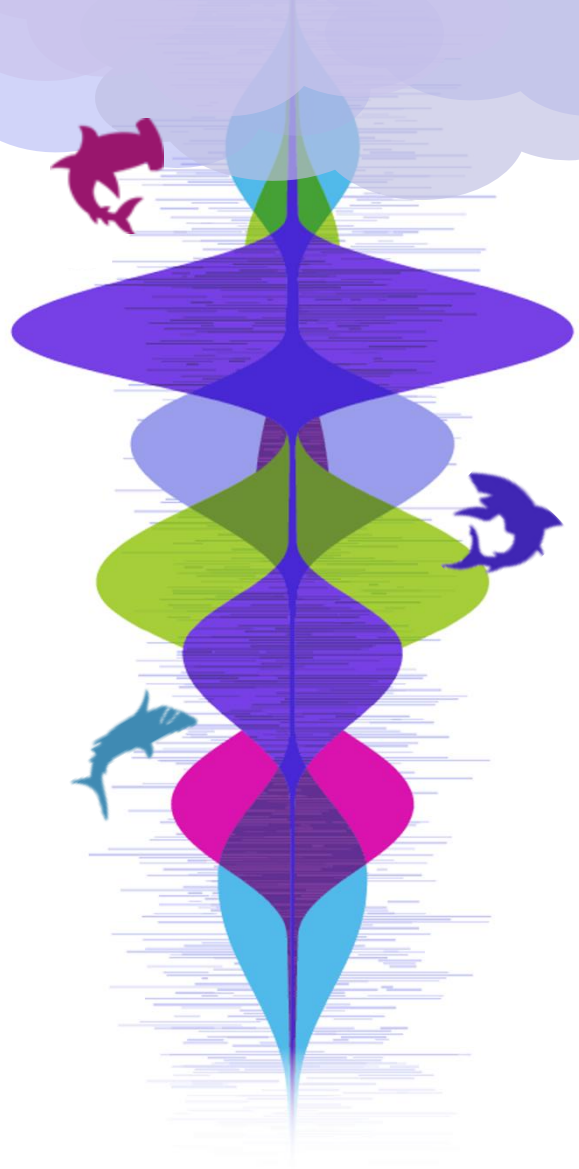
for orgs with high level of noncompliance

Target's Solution:

Enterprise Incident Management

Agenda

- **The Enterprise Incident Mgmt Team**
  Who the team is and what it needs
- **The Cross-Functional Support**
  Expertise at the right level
- **The Incident Mgmt Framework**
  Core elements to build upon
- **The Team in Action**
  Real life example
- **Q&A**



RSAC 2025 Conference

Part 1:
The Enterprise Incident Mgmt Team

What the team does

Coordinate *Lead the War Room*

Communicate *Control the messaging*

Escalate *Bring the right visibility*

Remediate *Drive through recovery*

Who the team is

- Curious
- Risk-Driven
- Organized
- Strong Communicators

- Network of Partners
- Sr. Leader Supported
- Recognized Top-Down

RSAC 2025 Conference

Part 2:
The Cross-Functional Support

Cross-Functional Support

What

A **CFT** that provides **support** and whose members are **accountable** for decisions within their functional areas

Who

Key representatives at the **right level** from the teams needed in high-severity incidents

How

Updated consistently, meets regularly, and **undergoes exercises** to maintain incident readiness

Our Approach

Teams Represented

Law
Communications
Reputation Mgmt
Physical Security
Financial Services
Internal Audit
Compliance & Ethics
CAO Controller
Government Affairs
Tech Ops Center

RSAC 2025 Conference

Part 3:
The Incident Mgmt Framework

You can’t plan for EVERYTHING…

You can't plan for EVERYTHING…

…so make your framework handle ANYTHING

Core Characteristics

Flexible

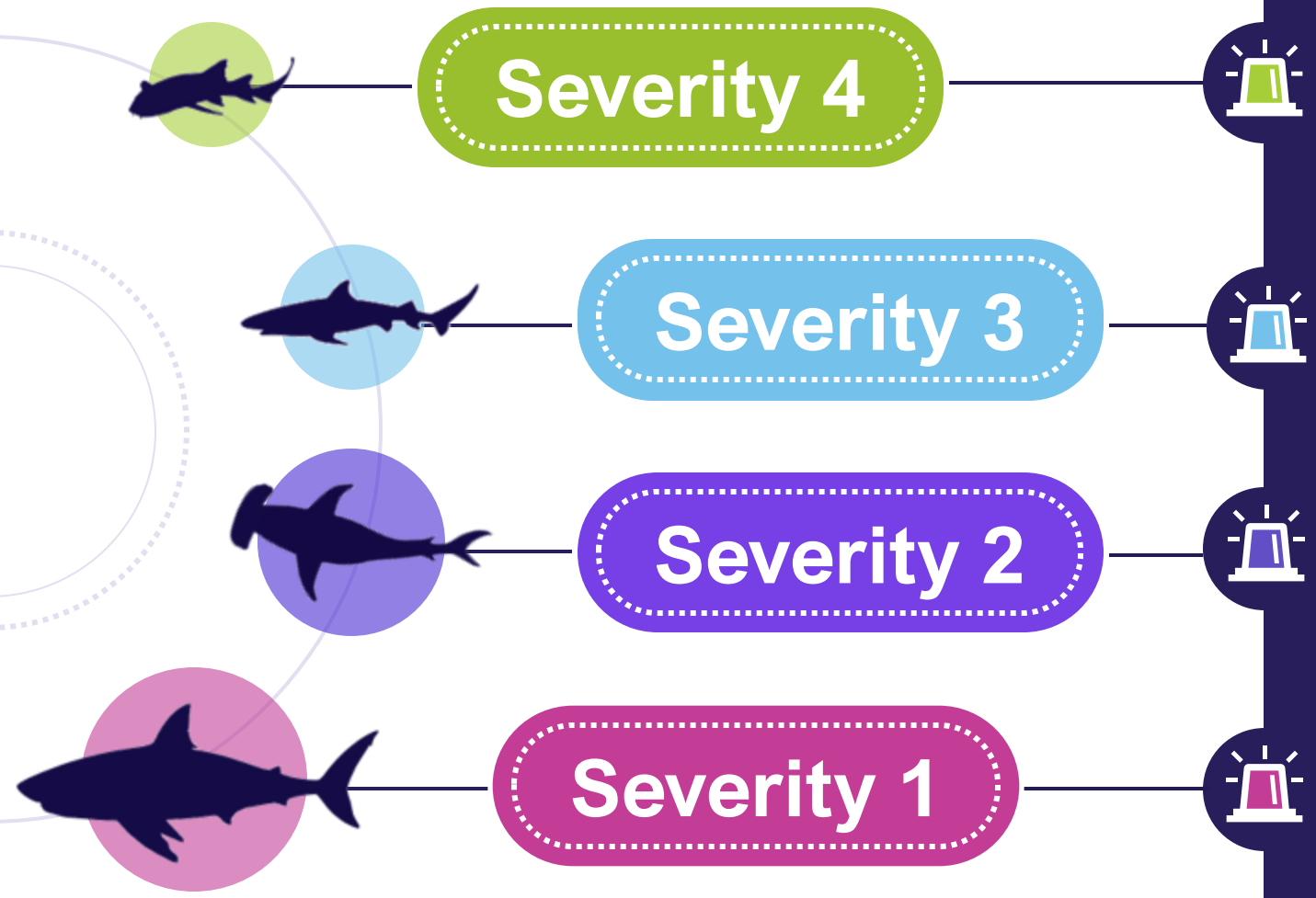
Living

Consumable

Well-Communicated

Core Components

Start with Severity Guidance



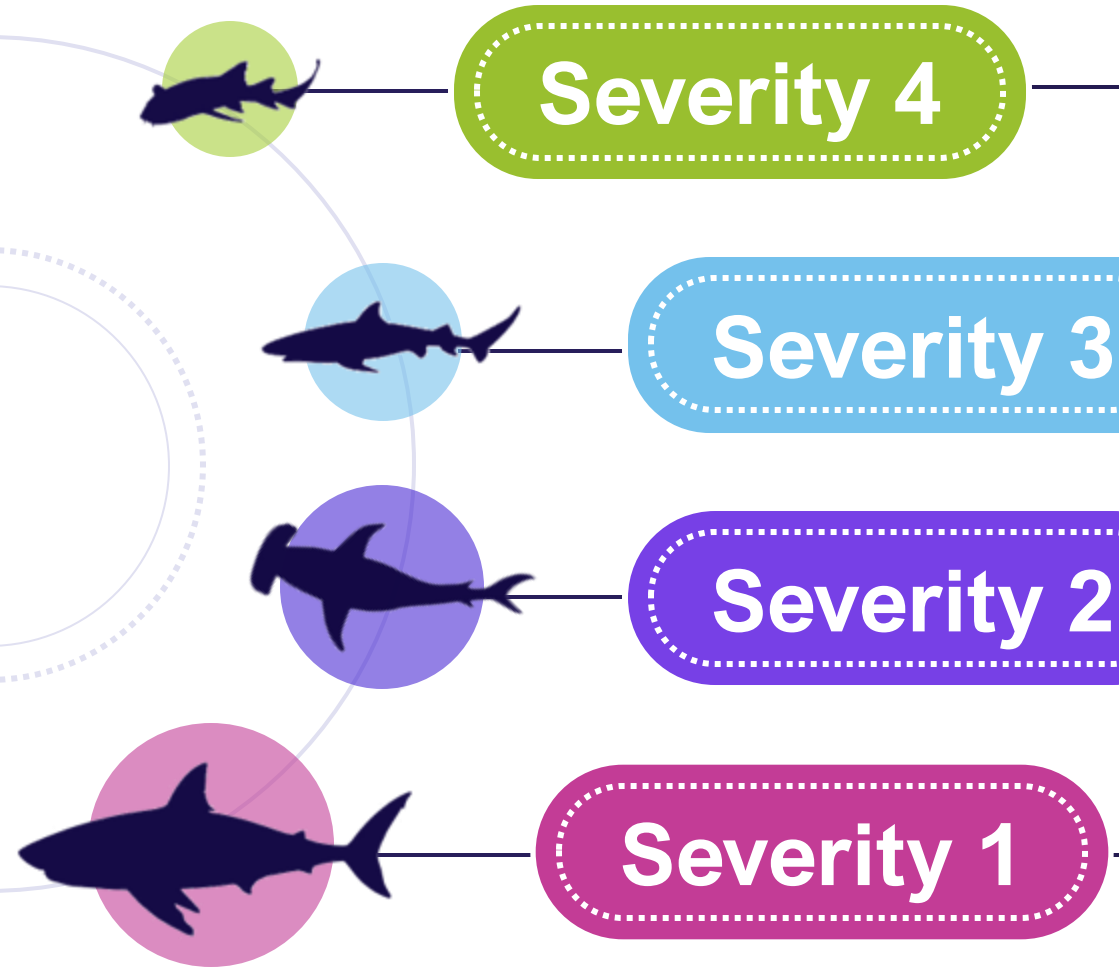
Team member installs **risky software** on their work laptop

Contracting vendor completely offline due to **ransomware attack**

Newly-discovered **Log4J** vulnerability impacts multiple **externally-facing** systems

2013 breach exposes card data of millions of guests

Layer In Escalation Model



Enterprise Incident Mgmt
Case Handlers

Core Incident Mgmt Team
Directors and Sr. Directors

Information Risk Council
Vice Presidents & Sr. VPs

LT Task Force
C-Suite Representatives

Add Supporting Processes

RSAC 2025 Conference

Part 4:
The Team in Action

How EIM Operates

BEFORE
Proactive Prep

Use **Threat Intel** to drive:

- Posture Improvements
- Red Lever Identification
- Exercise+Playbook Creation

DURING
Triage, Contain, Recover

Activate the War Room

Engage SMEs

Assign Action Items

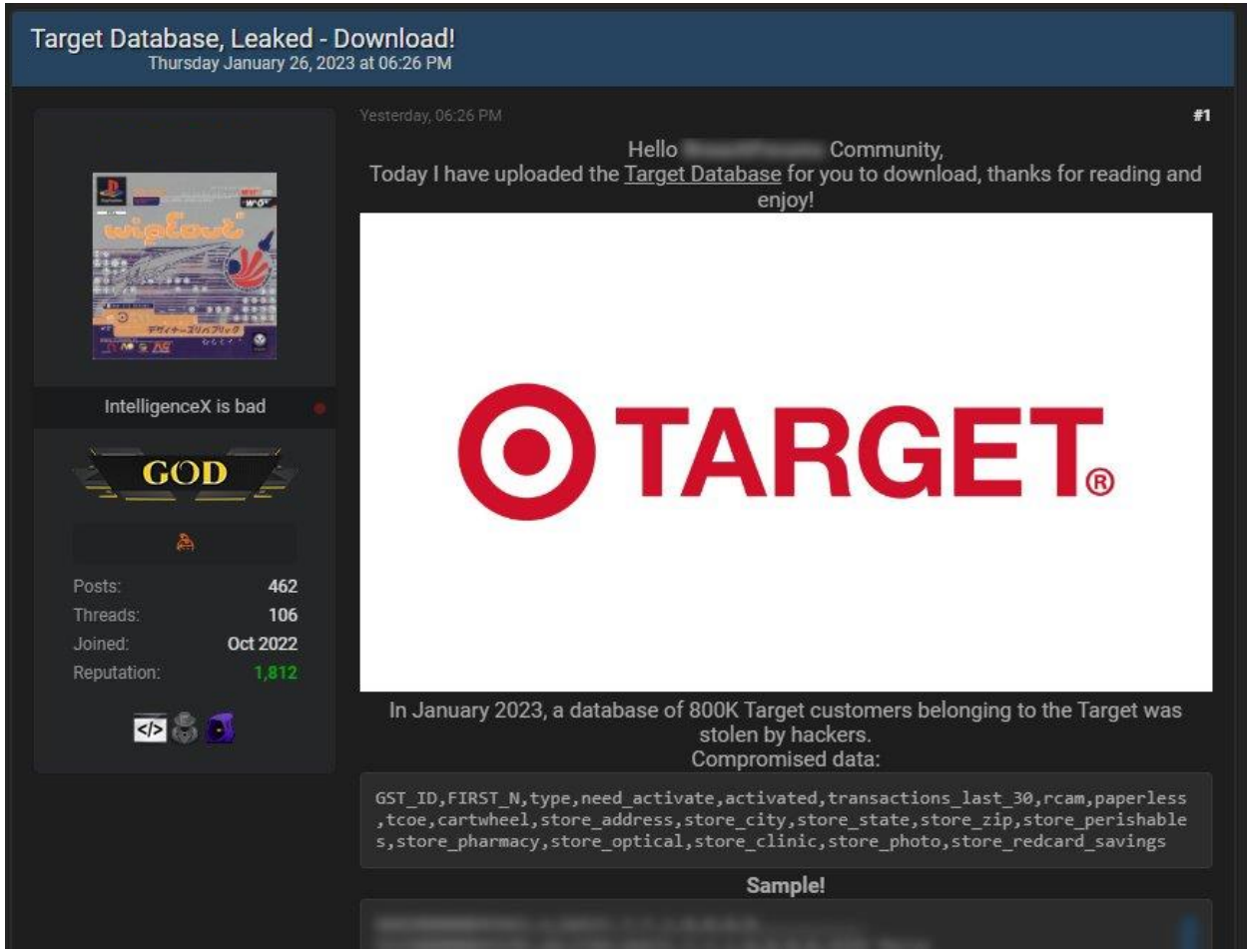
Communicate Updates

AFTER
Learn and Grow

Run **After Action Reviews** to:

- Identify gaps and friction
- Improve processes
- Document & track risks

Alert: Thursday Morning


Target Database, Leaked - Download!
Thursday January 26, 2023 at 06:26 PM
Yesterday, 06:26 PM
#1
Hello [redacted] Community,
Today I have uploaded the Target Database for you to download, thanks for reading and enjoy!
IntelligenceX is bad
GOD
Posts: 462
Threads: 106
Joined: Oct 2022
Reputation: 1,812
TARGET
In January 2023, a database of 800K Target customers belonging to the Target was stolen by hackers.
Compromised data:
GST_ID,FIRST_N,type,need_activate,activated,transactions_last_30,rcam,paperless,tcoe,cartwheel,store_address,store_city,store_state,store_zip,store_perishables,store_pharmacy,store_optical,store_clinic,store_photo,store_redcard_savings
Sample!

EIM Engaged

War Room Established

Alert: Thursday Morning

Data Exfil Claims – Severity 2

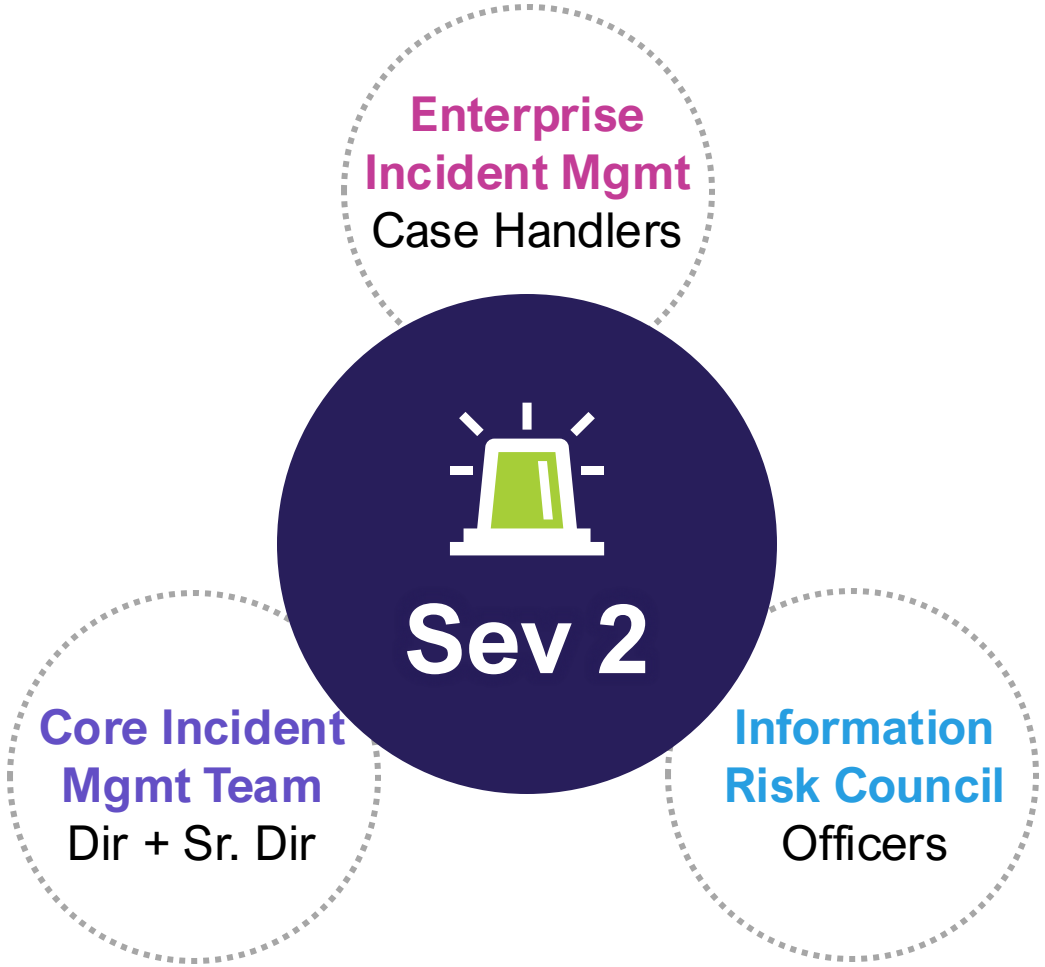
What We Know

- TA claims to have stolen DB w/ **800K records**
- Data are **not PII or sensitive** and also **highly outdated**
- Threat actor has recently made **similar claims** for other large companies

Action Items

- ❑ Scope env for data
  - ❑ Asset scans (CSIRT)
  - ❑ Network traffic review (CSIRT)
  - ❑ Engage SMEs familiar with data (EIM)
- ❑ Monitor for media attention (Comms)
- ❑ Connect with peers (CTI)

Escalation: Thursday Afternoon



Law confirms data exposure **does not** require notification

Comms, R&R, and Law begin preparing **media statement**

Financial Services rep provides **SMEs** to assist with scoping

Continued Scoping: Thursday Night

Sources Searched

- Network traffic
- Cloud storage
- File shares
- Big data storage
- Asset Scans

Teams Engaged

- RedCard
- Financial Services
- Digital
- Guest Services
- CCPA

Conclusion:

Data not taken from our environment

Case Sync: Friday Morning

Data Exfil Claims - Severity 2

What We Know

- TA claims to have stolen DB w/ **800K records**
- Data are **not PII or sensitive** and also **highly outdated**
- Threat actor has made **similar claims** for other large companies recently

Action Items

- ✓ Scope environment for similar datasets - *Complete, high confidence data did not come from our env*
- ✓ Review network traffic for exfil - *Complete - none seen*
- ✓ Monitor for media attention - *Request for comment from The Record, statement updated and sent*

Reaction: Friday Afternoon

Jonathan Greig

January 27th, 2023

Briefs | Cybercrime

Target says data sold on dark web is 'outdated,' likely 'released by third party'

After Action: The Following Week

What could have been improved?

- Update vendor data retention agreements
- Improve detection on Dark Web posts
- Turn actions taken into a runbook for data sweeps

RSAC 2025 Conference

Part 5: Apply

Apply

- **Next week you should:**
  - Evaluate current teams and processes to start building a plan to staff an EIM function
- **In the first three months following this presentation you should:**
  - Identify key partners needed to provide cross-functional support
  - Draft severity definitions and escalation processes
- **Within six months you should:**
  - Take your plan and obtain top-down buy-in
  - Layer in key playbooks and process guides
  - Plan an exercise to test what you've built

RSAC™ 2025 Conference

Many Voices.
One Community.

For more information, contact

Sydney.DeIp@target.com